

SEZIONE 25

SMD VI – CAP. 7120-02

1. PREMESSA

Ai sensi dell'articolo 548 comma 1 sotto commi b, c, del Decreto Legislativo 15 marzo 2010 n. 66, la relazione riferisce sullo stato di attuazione dei programmi dello Stato Maggiore Difesa – VI Reparto relativi al capitolo 7120-02 realizzati nel 2020.

2. ILLUSTRAZIONE DELLO STATO DI ATTUAZIONE DEI PROGRAMMI

a. Programmi di investimento finanziati con bilancio ordinario

I programmi riguardano l'adeguamento del sistema radio avionico ed il sistema ricetrasmittente navale/terrestre, ed il potenziamento del sistema informativo gestionale per la gestione tecnico/logistica dei velivoli ad ala rotante.

(1) PROGRAMMA SATURN

L'impresa, avviata nel corso del 2019, si pone l'obiettivo di adeguare il sistema radio avionico nelle bande di frequenza V/UHF (mod. RT 651/N-S) ed il sistema ricetrasmittente navale/terrestre (mod. RT 619/NV), in linea con il nuovo "UHF *Allotment Plan*" definito nell'ambito della c.d. UHF *Reorganization* della NATO, per consentire la piena interoperabilità e protezione delle comunicazioni militari tattiche, secondo i relativi standard (i.e. STANAG 4372). Il programma, gestito dalla Direzione Tecnica di ARMAEREO, prevede la conclusione delle attività di sviluppo a cura della Società LEONARDO entro la fine del 2021, per un onere complessivo per l'A.D. di circa 2,4 M€ (interamente speso su territorio nazionale).

L'importo a carico della Difesa è stato di circa 0.97M€.

(2) POTENZIAMENTO/AGGIORNAMENTO FUNZIONALITA' SISTEMA SILEF

Lo Stato Maggiore della Difesa ha avviato nel corso del 2018 un progetto che prevede l'impiego del Sistema Informativo Logistico Efficienza (SiLEF), in uso presso l'Aeronautica Militare, quale sistema informativo gestionale per la completa gestione tecnico/logistica dei velivoli ad ala rotante.

Con le attività già finanziate nel corso dei precedenti esercizi finanziari è stato possibile implementare il sistema in parola a favore degli Enti pilota di EI e MM.

Con il completamento delle verifiche di raggiungibilità del servizio e l'installazione delle prime postazioni del SiLEF, si è inteso acquisire il supporto specialistico necessario a garantire alle Forze Armate la disponibilità di specifiche figure professionali per il consolidamento delle attività di caricamento dei dati relativi alla *master configuration* degli assetti individuati (CH47F/Esercito e EH101/Marina) e, successivamente, l'utilizzo delle funzionalità aeronautiche anche dal punto di vista della gestione del personale (mantenimento in *currency*, idoneità al volo, abilitazioni, visite mediche, ecc.).

L'importo a carico della Difesa è stato di 0.5M€.

b. Quadro sinottico dei programmi

In Tabella 26 al presente allegato è riportato il quadro riepilogativo dello stato di attuazione dei programmi sopra riportati.

3. RAPPORTO TRA SPESE IN ITALIA E ALL'ESTERO

Il programma nel corso del 2020 ha avuto un onere complessivo **1,47M€**.

SEZIONE 26

SMD VI - CAP. 7120-03

1. PREMESSA

Ai sensi dell'articolo 548 comma 1 sotto commi b, c, del Decreto Legislativo 15 marzo 2010 n. 66, la relazione riferisce sullo stato di attuazione dei programmi dello Stato Maggiore Difesa – VI Reparto relativi al capitolo 7120-03 realizzati nel 2020.

2. ILLUSTRAZIONE DELLO STATO DI ATTUAZIONE DEI PROGRAMMI

a. Programmi di investimento finanziati con bilancio ordinario

I programmi riguardano l'acquisizione di sistemi radio satellitari e TBT per il comparto delle operazioni speciali per poter esercitare in maniera efficace e tempestiva la direzione di un'operazione militare nell'ambito dell'assolvimento dei compiti di istituto della Difesa e in attività Fuori Area (Operazione *InherentResolve* IRAQ).

(1) AMMODERNAMENTO\ADEGUAMENTO RETI TELEMATICHE (C4I Difesa)

Il comparto delle Forze Speciali è impegnato in attività operative nazionali ed internazionali in cui la complessità dell'ambiente richiede la disponibilità di un sistema CIS a livello tattico, efficace e ad alto contenuto tecnologico in grado di assicurare la piena integrazione nell'architettura *netcentrica* dello strumento militare. In tale contesto si inseriscono gli assetti Radio Satellitari UHF oggetto di acquisizione, che permettono di realizzare collegamenti terra-bordo-terra con capacità satellitare tattica in grado di garantire il flusso di informazioni voce e dati in maniera affidabile e classificata.

L'importo a carico della Difesa è stato di circa 0,075M€.

b. Quadro sinottico dei programmi

In Tabella 27 al presente allegato è riportato il quadro riepilogativo dello stato di attuazione dei programmi sopra riportati.

3. RAPPORTO TRA SPESE IN ITALIA E ALL'ESTERO

Il programma nel corso del 2020 ha avuto un onere complessivo **0,075M€**.

SEZIONE 27

SMD VI - CAP. 7120-04

1. PREMESSA

Ai sensi dell'articolo 548 comma 1 sotto commi b, c, del Decreto Legislativo 15 marzo 2010 n. 66, la relazione riferisce sullo stato di attuazione dei programmi dello Stato Maggiore Difesa – VI Reparto relativi al capitolo 7120-04 realizzati nel 2020.

2. ILLUSTRAZIONE DELLO STATO DI ATTUAZIONE DEI PROGRAMMI

a. Programmi di investimento finanziati con bilancio ordinario

I programmi riguardano la realizzazione di infrastrutture di comunicazione strategica, satellitare ed in fibra ottica, che consentono di acquisire capacità essenziali di Comando, Controllo, Comunicazione, Computer necessarie per poter esercitare in maniera efficace e tempestiva la direzione di un'operazione militare nell'ambito dell'assolvimento dei compiti di istituto della Difesa e in attività Fuori Area.

(1) SISTEMI C4I DIFESA

Diversi programmi, sia a carattere annuale sia pluriennale, concorrono all'adeguamento ed al potenziamento di questo settore strategico attraverso molteplici attività concorrenti ad assicurare alla Difesa le disponibilità di capacità funzionali allo svolgimento di operazioni interforze ed internazionali; tra i programmi di maggior rilievo si segnalano:

a) Contratto 10068 di Rep del 23/12/2011 relativo allo sviluppo ed acquisizione di Cifranti di nuova generazione e nuovi algoritmi di cifratura

Il programma ha la finalità di ammodernare il settore delle comunicazioni IP cifrate, attraverso lo sviluppo e acquisizione di 300 moderni apparati in grado di utilizzare nuove famiglie di Algoritmi di Cifratura, che garantiscano elevate velocità di trasmissione, l'interoperabilità con *standard* e protocolli già in uso/di concordata introduzione in ambito NATO (NINE). L'obiettivo è quello di assicurare lo scambio di dati classificati, così come imposto dai moderni scenari di impiego. Il programma nel corso del 2020 ha avuto un onere complessivo di 2,6M€

b) Piano di realizzazione del parco infrastrutturale ubicato in Roma – Predisposizione CIS per la fruizione dei servizi ICT classificati e non classificati dell'AVI

Il progetto ha lo scopo di gestire in maniera accentrata, garantendo l'estensione dei servizi non classificati della Difesa (Posta Elettronica, Documentale, Gestione della Policy di sicurezza, etc.), tutti quegli Enti, Distaccamenti, Reparti e Comandi (EDRC) dell'Area di Vertice della Difesa che ancora erano gestiti con un proprio dominio a livello locale.

Il Centro di Dematerializzazione e Conservazione Unico della Difesa (Ce.De.C.U.), realizzato presso l'ex Stabilimento Grafico Militare di Gaeta, ha acquisito la piena capacità di "Dematerializzazione" dei documenti cartacei e della loro "Conservazione" nel tempo in formato digitale. Tale Centro ha anche conseguito, da parte dell'Agenzia per l'Italia Digitale (AgID), la certificazione quale "Conservatore Accreditato", necessaria per poter fornire tale servizio ad Enti esterni (sia P.A. che privati).

Tale attività ha comportato un adeguamento ed una standardizzazione dei materiali *hardware* e di Postazioni di Lavoro, nonché supporto di personale specializzato. Il programma nel corso del 2020 ha avuto un onere complessivo di circa 0,3M€.

c) So.Fu.Tra. 2019 – Interforze – DII – Potenziamento della sicurezza informatica e protezione cibernetica dell’End Point. Acquisizione centralizzata del S.O. Win 10 e Advanced Threat Analytics (ATA).

Nell’ottica di garantire univocità di indirizzo e coerenza d’azione nel settore ICT, si sta perseguendo, già da tempo, sia un’opera di standardizzazione e di crescita del livello di interoperabilità dei sistemi e delle applicazioni informatiche gestionali, inclusi gli aspetti di sicurezza (dei dati e delle reti), sia iniziative finalizzate al contenimento degli oneri finanziari attraverso una centralizzazione della spesa.

Inoltre, nell’ambito delle attività connesse con il potenziamento della sicurezza informatica e protezione cibernetica della DII, si è dotato il dominio della Difesa di uno strumento per l’analisi, l’interpretazione e la correlazione delle informazioni relative alle attività svolte dagli utenti e conservate nel servizio di *directory* denominato *Advanced Threat Analytics (ATA)*.

Il programma nel corso del 2020 ha avuto un onere complessivo di circa 6,5M€.

d) Software Defined Radio - Avio (SDR-AVIO)

L’impresa si inquadra in continuità con il C.tto nr. 9940 di rep. del 30.06.2011, precedentemente avviato dall’A.D. per lo sviluppo di sistemi radio basati su tecnologia Software Defined Radio (SDR). Il programma SDR AVIO ha l’obiettivo estendere l’impiego di piattaforme SDR sui velivoli ad ala fissa e rotante in dotazione alle F.A., in grado di supportare sia le modalità di comunicazione c.d. legacy che le future comunicazioni Air to Ground e Air to Air. Il programma, gestito dalla Direzione Tecnica di TELEDIFE, prevede la conclusione delle attività di sviluppo e qualifica, a cura della società LEONARDO entro il 2022, per un onere complessivo per l’A.D. di circa 3M€ (spesa interamente sostenuta in territorio nazionale).

Il programma nel corso del 2020 ha avuto un onere complessivo di circa 0,3M€.

e) ESSOR (European Security Software Radio)

ESSOR (European Secure Softwar Radio) è un’iniziativa di cooperazione europea per sviluppi basati su tecnologia Software Defined Radio (SDR) per le comunicazioni militari tattiche. Inizialmente costituita da 6 nazioni (Finlandia, Francia, Italia, Polonia, Spagna, Svezia), la cooperazione si è allargata nel mese di dicembre 2019 con l’adesione della Germania. Il programma mira allo sviluppo di un’architettura SDR comune europea ed allo sviluppo di forme d’onda (al momento la c.d. High Data Rate Waveform - HDR WF) da proporre come standard di interoperabilità a livello Unione Europea e NATO. Il programma è gestito dall’agenzia internazionale OCCAR-EA, in qualità di Programming e Contracting Authority, ed è affidato ad un consorzio industriale denominato “A4ESSOR”, composto dalle principali realtà produttive dei paesi partecipanti¹.

Il programma nel corso del 2020 ha avuto un onere complessivo di 3,5M€.

f) Enterprise Agreement con la Società Environmental System Research Institute (ESRI) Incorporate

La società ESRI è un’Azienda di rilevanza internazionale e leader nel settore GIS (Geographic Information System); i prodotti forniti da ESRI sono attualmente impiegati in modo massiccio nell’ambito dei principali sistemi C2 ed ISTAR nazionali di livello tattico, operativo e strategico. Inoltre, diverse articolazioni della Difesa e la totalità delle Forze Armate hanno in itinere attività di sviluppo su sistemi specialistici o di combattimento basati su prodotti forniti in ambito AQ (Accordo Quadro).

In particolare gli applicativi ESRI sono stati impiegati per:

¹ INDRA (ESP), BITTIUM (FIN), THALES (FRA), LEONARDO (ITA), RADMOR (POL) e SAAB (SWE), Rohde & Schwartz (GER)

- gli sviluppi del SIACCON ADV e del SICCONA, nell'ambito del Programma Forza NEC (FNEC);
- l'implementazione del Sistema di Combattimento SADO 4 delle nuove piattaforme della Marina Militare già varate e in corso di progettazione nell'ambito della "Legge Navale";
- l'impiego e il mantenimento nel ciclo di vita del Sistema C2I Difesa ADV, impiegato quale sistema joint per la generazione della *Common Operational Picture* dal Comando Operativo di Vertice Interforze (COI) e dal NATO *Rapid Deployable Corps - Italy* (NRDC-ITA). In particolare più aggiornati *server* cartografici sono stati impiegati per la realizzazione della nuova versione del C2I-ADV 2.0

Risultano, inoltre, sviluppati su prodotti ESRI, con risorse di assistenza sistemistica tratte dall'AQ i seguenti prodotti:

- la piattaforma MARTINA (*Management of Rasters, videos and layers for multi-Temporal Intelligence Analysis*), per la gestione del ciclo IMINT del Centro *Intelligence* Interforze;
- il portale GEOSPAZIALE della Difesa, e implementato sotto la guida del II Reparto di SMD (RIS PIGE);
- i portali geospaziali delle F.A., attualmente in fase embrionale, che verranno popolati con i prodotti cartografici degli Enti specialistici delle singole Forze Armate (Istituto Geografico Militare dell'Esercito, Istituto Idrografico della M.M. e Centro Informazioni Geotopografiche Aeronautiche) e che, federati con il portale AURORA, consentiranno di creare, gestire e distribuire servizi cartografici a supporto di tutte le aree della Difesa;
- il portale GEORETI della Difesa, attualmente in fase prototipale, per la raccolta delle informazioni relative alle infrastrutture telematiche, ai fini di programmazione delle reti.

Lo sviluppo dei programmi sopra indicati con tecnologia ESRI, che di fatto costituisce uno standard, adottato anche in ambito NATO, semplifica l'implementazione di profili di interoperabilità sia in ambito nazionale che con gli analoghi sistemi sviluppati in ambito Coalizione; allo stesso tempo, garantisce un livello di standardizzazione che rende più agevole lo sviluppo di una governance unificata con conseguente riflesso positivo nel supporto alle attività operative.

Alla luce di tale ampio impiego dei prodotti e servizi della Società ESRI, l'A.D. ha proceduto alla definizione di un Accordo Quadro triennale che consente di conseguire ingenti vantaggi e risparmi in termini di costo di manutenzione e rinnovo licenze e costo di supporto sistemistico e addestrativo per il personale della Difesa. Il programma nel corso del 2020 ha avuto un onere complessivo di circa 0,49M€, quota impegnata per intero sul territorio nazionale.

g) *Business Continuity e Disaster recovery* servizi informativi gestionali CED Area di Vertice Interforze – Fase 1B - - Avvio e Completamento

Nell'ambito del piano di razionalizzazione del parco infrastrutturale, è in corso una fase di consolidamento dei servizi del Segretariato Generale della Difesa/Direzione Nazionale degli Armamenti (SGD/DNA) e delle dipendenti Direzioni Tecniche presso i data center del Comando C4 Difesa e di "Palazzo Guidoni" c/o l'Aeroporto Militare di Centocelle. In tale contesto sussiste la necessità di acquisire hardware e software per consentire il ricollocamento dei citati servizi, incluso il framework di sicurezza e di networking. Il progetto si basa su più fasi:

- Fase 1 – Acquisizione di *hardware* di nuova generazione sui sedimi del C4D e SEGREDIFESA con relativa implementazione di servizi di virtualizzazione di due *data center*;
- Fase 1b – Progettazione:
 - della ricollocazione dei servizi erogati dai CED di Segredifesa ubicati presso l'infrastruttura di via Marsala di Roma e Palazzo Messe sede di PERSOMIL;

- della realizzazione del DR nella sede di Padova;
- della realizzazione del *Private Cloud* della Difesa.

Il programma nel corso del 2020 ha avuto un onere complessivo di 0,736M€.

h) Acquisizione centralizzata licenze e servizi ORACLE per SMD, SGD e FA

Il programma ha la finalità di acquisire licenze software in modalità unlimited e servizi professionali volti a favorire la standardizzazione delle piattaforme database da utilizzare nei diversificati sistemi informatici della Difesa, utilizzando prodotti della Società ORACLE.

Il programma nel corso del 2020 ha avuto un onere complessivo di 1,9M€.

i) NGIFF

La Difesa, allo scopo di rendere pienamente interoperabili gli assetti terrestri, navali e aerei delle F.A. sia in ambito nazionale che in quello NATO, ha avviato l'aggiornamento dei sistemi per l'identificazione tattica Aria-Aria (A-A) e Superficie-Aria (S-A) (cosiddetta capacità di Identification Friend or Foe - IFF) allo STANAG 4193 Ed. 3, per i modi militari, ed ai Documenti ICAO (Annesso 10 Amendment 85), per quelli civili. Il programma ha lo scopo di sviluppare i kit retrofit dei capi serie dei sistemi IFF (transponder/interrogatori) di produzione nazionale, in modo da consentire, con successive attività contrattuali, l'aggiornamento di tutti gli assetti delle F.A. dotati della citata capacità di identificazione e riconoscimento.

Il programma nel corso del 2020 ha avuto un costo di circa 2,9M€, quota impegnata quasi esclusivamente per intero sul territorio nazionale

j) Acquisizione centralizzata di licenze VMWARE per federazione Cloud della DIFESA

Il programma ha la finalità di acquisire licenze software e crediti da utilizzare nel triennio di validità del Contratto Quadro. Mediante tali crediti il Comparto difesa può acquisire o ulteriori licenze software o servizi professionali volti necessari allo studio e sviluppo di progetti basati su tecnologia VMware. Tra i progetti di interesse Strategico vi è l'implementazione del Community Cloud, su cui far convergere parte dei applicativi di FA, al fine di razionalizzare risorse tecnologiche ed economiche, ottemperando alla disposizione dell'accorpamento dei vari CELD.

Il programma nel corso del 2020 ha avuto un costo di 2,9M€.

k) EVOLUZIONE SCIP

L'impresa ha l'obiettivo di ammodernare le capacità del sistema "SCIP - Rete Difesa" per le comunicazioni sicure, prevedendo lo sviluppo e la fornitura di nuovi terminali di telefonia fissa e mobile abilitati (fino a livello RISERVATO), in accordo al Secure Communications Interoperability Protocol. Il programma, gestito dalla Direzione Tecnica di TELEDIFE, prevede la conclusione delle attività di sviluppo e certificazione a cura del consorzio industriale LEONARDO- TELSYP entro il 2022, per un onere complessivo per l'A.D. di circa 1,9M€.

Il programma nel corso del 2020 ha avuto un costo di circa 0,4M€.

l) DISTRIBUTION LAYER DELLA MAN DI ROMA

La rete telematica Metropolitana dell'area romana è strutturata, come da best practice del settore, in differenti layer, ciascuno dedicato a diverse funzionalità. Allo scopo di prevenire l'obsolescenza e, soprattutto, incrementare la protezione cibernetica della rete che veicola servizi ICT all'Area di Vertice Interforze e delle F.A., è in corso un programma per l'ammodernamento degli apparati attivi che realizzano il distribution layer. Attualmente è stato completato oltre il 90% dell'ammodernamento in parola.

Il programma nel corso del 2020 ha avuto un costo di circa 0,4M€.

m) RIFON - COMPLETAMENTO/ADEGUAMENTO BACKBONE E CODE DI F.A. DI RILEVANZA INTERFORZE

La Rete Interforze in Fibra Ottica Nazionale (RIFON) è la principale infrastruttura di comunicazione che compone la Rete Integrata della Difesa, in quanto, essa è massivamente estesa sul territorio nazionale, trasporta a banda larga tutti i servizi ICT Interforze e delle F.A. necessari alle attività operative, logistiche e amministrative dell'intero Comparto. Questa complessa infrastruttura ha bisogno di continui aggiornamenti per non perdere il contatto con lo "stato dell'arte" tecnologico e di estensioni delle tratte, per elevare la resilienza e/o raggiungere il maggior numero possibile di siti della Difesa. In particolare, nel 2020 si sono conclusi i lavori riguardanti:

- l'ammodernamento degli apparati fotonici di rete, che illuminano i collegamenti ottici sottomarini tra la penisola italiana e le isole maggiori;
- l'acquisizione del *server* per la cifratura *on-line* (algoritmo commerciale) delle future connessioni in fibra ottica ad alta capacità (c.d. *lambda* DWDM ROADM);
- l'ammodernamento delle stazioni di energia obsolescenti dedicate all'alimentazione elettrica in continuità dei nodi TLC della stessa RIFON;
- la realizzazione della nuova dorsale ottica tra Bari e Lecce;
- la realizzazione di nuovi collegamenti ottici per raggiungere varie sedi dell'Area interforze e della M.M..

Il programma nel corso del 2020 ha avuto un costo di circa 1,5M€.

n) ADEGUAMENTO CAPACITA' COMPUTAZIONALI E DI STORAGE – CITRIX

Il presente programma di acquisizione ha l'obiettivo di adeguare le capacità computazionali e di storage del datacenter del Comando per le Operazioni di Rete allo scopo di implementare la soluzione di VDI (infrastrutturale e applicativa) di Citrix per verificare il corretto funzionamento e le performance delle componenti sia DataCenter sia applicative (apparati di rete, utenti, postazioni di lavoro, servizi, ecc.) presenti in ambito SMD.

In particolare, con il presente programma si vogliono acquisire l'hardware e il software di base necessario all'implementazione di una infrastruttura che:

- estenda i livelli funzionali e prestazionali dell'attuale infrastruttura a supporto della piattaforma VDI Citrix;
- rispetti i requisiti di segregazione e compartimentazione definiti nell'ambito del progetto *Cyber Defence Capability* fase 2;
- faciliti l'incremento delle capacità di *smart-working* offerto al personale della Difesa favorendo la remotizzazione delle applicazioni utente connessi con l'infrastruttura di rete e applicativa attualmente disponibile presso il Comando per le Operazioni di Rete.

Il programma nel corso del 2020 ha avuto un costo di circa 0,5M€.

o) EVOLUZIONE TECNOLOGICA FIRMA E IDENTITA' DIGITALE DELL'A.D. – PKI/CMS E FUNZIONALITA' STRONG AUTHENTICATION

L'obiettivo del presente programma è quello di circostanziare l'esigenza della Difesa per il mantenimento in garanzia della componente *hardware* e *software* di base dell'infrastruttura PKI e CMS e le relative attività di supporto specialistico al fine di:

- garantire la corretta funzionalità dell'infrastruttura PKI e CMS Unico;
- condurre le attività evolutive per garantire al Sistema l'aderenza ai vincoli normativi nazionali ed europei necessari a mantenere la certificazione dell'infrastruttura di cui si è dotata la Difesa preposta all'emissione del modello ATe e ai certificati digitali ad esso associati attraverso la propria *Certification Authority* a favore di tutto il personale della Difesa e delle Amministrazioni Pubbliche che hanno stipulato con quest'ultima un Accordo di collaborazione;
- ammodernare la componente *hardware* e *software* della PKI sia nel sito primario presso il Comando per le Operazioni in Rete che nel sito secondario di *Disaster Recovery* (DR) presso il *Card Management System* Unico ospitato nel Comando C4 Esercito (ovvero presso il costituendo sito di BC/DR di Centocelle). Il supporto dovrà garantire sia l'utilizzo di apparati "aggiornati tecnologicamente" sia dei certificati per l'utilizzo di sistemi operativi, aumentare la capacità di archiviazione dei dati

dell'infrastruttura (ciclo di vita certificati, marche temporali, giornali di controllo, log dei sistemi ecc);

- mantenere aggiornato il *software* di base dell'infrastruttura PKI.

Il programma nel corso del 2020 ha avuto un costo di circa 0,5M€.

b. Quadro sinottico dei programmi

In Tabella 28 al presente allegato è riportato il quadro riepilogativo dello stato di attuazione dei programmi sopra riportati.

3. RAPPORTO TRA SPESE IN ITALIA E ALL'ESTERO

In totale, per il capitolo 7120-04, sono stati spesi circa **27,8M€** interamente in ambito nazionale.

SEZIONE 28

SMD VI - CAP. 7120-23

1. PREMESSA

Ai sensi dell'articolo 548 comma 1 sotto commi b, c, del Decreto Legislativo 15 marzo 2010 n. 66, la relazione riferisce sullo stato di attuazione dei programmi dello Stato Maggiore Difesa – VI Reparto relativi al capitolo 7120-23 realizzati nel 2020.

2. ILLUSTRAZIONE DELLO STATO DI ATTUAZIONE DEI PROGRAMMI

a. Programmi di investimento finanziati con bilancio ordinario

Trattasi di programmi volti ad ammodernare/mantenere/adequare i sistemi di comunicazione e di Comando e Controllo della componente strategica della Difesa e dei Comandi Interforze all'evoluzione tecnologica.

(1) CYBER DEFENCE CAPABILITY

a) LDB 2017 – Art. 1 co 140 – Rinnovamento *Cyber Defence Capability* – DII – Progetto *Cyber Lab*

Il programma ha l'obiettivo di acquisire gli strumenti necessari a realizzare i principali ambienti operativi del Comando Interforze per le Operazioni Cibernetiche (CIO), nell'ambito dei quali effettuare analisi tecniche e verifiche *post* incidente informatico, *reverse engineering* sui *malware*, analisi tecnica per la identificazione di Tecniche Tattiche e Procedure (TTP) avversarie, ricerca di indicatori di compromissione e supporto alla progettazione di reti *secure by design*, specifiche per le info-strutture della Difesa, nonché sviluppo e sperimentazione di assetti *cyber* e delle relative TTP per il loro impiego nell'ambito delle possibili operazioni militari cibernetiche nei Teatri Operativi secondo le RoE e le norme in vigore.

Il programma nel corso del 2020 ha avuto un onere complessivo di 0,21M€

b) LDB 2017 – Art. 1 co 140 – Rinnovamento *Cyber DII* Potenziamento dei Servizi Professionali di analisi della minacce *cyber* e (*Threat Intelligence Service* - TIS).

Basandosi sull'esperienza maturata nel campo dell'analisi del *Cyber Threat* e sulle possibili evoluzioni della minaccia nel dominio cibernetico, SMD dal 2018 ha dato avvio all'acquisizione del servizio TIS, con l'obiettivo di dotare sia il *Computer Emergency Response Team* (CERT) della Difesa istituito presso il Comando Interforze Operazioni Cibernetiche (CIO), sia i SOC/CIRT (*Security Information Centre / Computer Incident Response Team*) del Comando C4 Difesa e delle F.A. degli elementi informativi necessari ad attuare un tempestivo contrasto dinamico della minacce *cyber* di imminente concretizzazione.

Il Servizio TIS è relativo al rilevamento e individuazione di nuove vulnerabilità, attacchi informatici in preparazione e informazioni sottratte illegalmente e pubblicate in rete, attraverso il controllo continuo delle fonti *web* e *darknet* e l'analisi in real-time di grandi quantità di dati alla ricerca di possibili indizi. È stato inizialmente acquisito a favore dell'area Interforze e dell'E.I. e nel 2019 è in corso di estensione anche a M.M. e A.M. e di potenziamento mediante l'integrazione di ulteriori fonti di *threat intelligence* e di

funzioni di investigazione aggiuntive specializzate sul servizio DNS (*Domain Name System*).

Il programma nel corso del 2020 ha avuto un onere complessivo di 3,2M€

c) LDB 2017 – ART.1 CO.140 – Rinnovamento *Cyber Defence Capability* - DII - estensione ITA *secret/restricted wan area* di vertice e stati maggiori/comandi operativi - 1^a QUOTA

Il programma si prefigge di proseguire il delicato processo di consolidamento e innalzamento dei livelli di *Cyber Security* della Difesa, previsto dal Libro Bianco, nonché mantenere l'*Information Superiority*, ampliando l'info-struttura dedicata alla gestione delle informazioni classificate dell'Area di Vertice/Comandi Operativi Interforze della Difesa.

Una più capillare diffusione di sistemi classificati, adeguatamente protetti e integrati da strumenti di *Cyber Defence*, incrementerà, inoltre, il livello di tutela dei dati sensibili e classificati in ambito A.D..

Il programma nel corso del 2020 ha avuto un onere complessivo di 0,38M€.

(2) AMMODERNAMENTO SISTEMI DI TELECOMUNICAZIONI ED INFORMATICA

a) LDB 2017 – art. 1 co. 140 – Rinnovamento *Cyber Defence Capability*. - certificazione del *Security Operation Center* (SOC)

Il programma ha l'obiettivo di supportare le attività di predisposizione necessarie a consentire al Security Operation Center (SOC) del Comando C4 Difesa di conseguire la Certificazione nell'ambito delle normative e framework internazionali applicabili nello specifico settore, in primis lo standard ISO 27001 per la sicurezza delle informazioni, con focus sulle misure minime di sicurezza dell'AgID e del GDPR. Le attività riguardano l'assessment sulla correttezza ed efficacia dei processi di gestione della sicurezza adottati dal SOC del C4D, l'implementazione di un Sistema di Gestione secondo le normative di settore e l'avviamento di un percorso di preparazione alla certificazione.

Il programma nel corso del 2020 ha avuto un onere complessivo di 0,645M€.

b) LDB 2017 – ART. 1 CO. 140 – Rinnovamento *Cyber Defence Capability*. – Acquisizione Capacità *CYBER* per pianificazione e condotta delle operazioni nel dominio cibernetico

Il programma ha l'obiettivo di acquisire sistemi in grado di fornire uno strumento di supporto decisionale al Comandante del CIOC, aiutandolo nella comprensione/valutazione dinamica del rischio di esposizione alla minaccia cyber, l'analisi e la scelta di possibili linee d'azione e l'attuazione tempestiva delle decisioni nella fase esecutiva delle operazioni cibernetiche finalizzate alla gestione/coordinamento della risoluzione degli incidenti, alla reazione ad attacchi cibernetici e al raggiungimento di obiettivi militari.

Il programma nel corso del 2020 ha avuto un onere complessivo di 4,2M€.

c) LDB 2017 – ART. 1 CO. 140 – Rinnovamento *Cyber Defence Capability* – Pianificazione e condotta delle operazioni nel dominio cibernetico - Acquisizione assetti per Cellule Operative Cibernetiche

Il programma è relativo all'acquisizione di assetti per le Cellule Operative Cibernetiche (COC), che il CIOC proietterà in teatro operativo in supporto al Comandante del Contingente, consentendogli di disporre della situational awareness nel dominio cyber e di pianificare e condurre operazioni militari nel dominio cyber.

Il programma nel corso del 2020 ha avuto un onere complessivo di 0,29M€.

d) LdB 2017 – Art. 1 co. 140 – DII – Rinnovamento *Cyber Defence Capability* – Strumenti per l’*Info-Sharing* nel Dominio cibernetico – Federazione dei SIEM.

Programma relativo alla federazione dei SIEM in dotazione all’area interforze e alle F.A., per la condivisione informativa (Information Sharing) sulle minacce ed attacchi cibernetici fra il CERT della Difesa, i SOC/CIRT2 delle F.A., l’esecuzione di analisi trasversali ai singoli ambiti di interesse; la valorizzazione delle storicizzazioni degli eventi cibernetici che ricorrono a medio termine (Collection and exploitation of historical data); la valorizzazione delle Lesson Learned sugli eventi informatici, anche per l’impiego in contesti esercitativi e di certificazione dell’approntamento delle forze. Il programma nel corso del 2020 ha avuto un onere complessivo di 1,07M€.

e) LdB 2017 – Art. 1 co. 140 – Esecuzione di interventi infrastrutturali e completamento GFE UNAVOX.

Programma connesso alla realizzazione poligono cyber (Progetto “Cyber Range”) presso la Scuola Telecomunicazioni delle FA a Chiavari.
Il programma nel corso del 2020 ha avuto un onere complessivo di 0,37M€.

f) LdB 2017 – Art. 1 co. 140 – Rinnovamento *Cyber Defence Capability* – Progetto “*Cyber Range*”

Il programma prevede la realizzazione, presso la Scuola Telecomunicazioni delle FA (STELMILIT) di Chiavari, di un poligono virtuale per la formazione e l’addestramento degli operatori e dei team da impiegare nel dominio cibernetico, la sperimentazione di nuove tecnologie di sicurezza, la partecipazione alle esercitazioni in ambito NATO/UE quale elemento federato nel network dei *cyber range*. La realizzazione del poligono *cyber* come assetto operativo impiegabile è ottenuto mediante l’allestimento dell’infrastruttura di supporto della piattaforma software sviluppata nell’ambito del progetto di ricerca tecnologica denominato UNAVOX.

Il programma nel corso del 2020 ha avuto un onere complessivo di 1M€.

b. Quadro sinottico dei programmi

In Tabella 29 al presente allegato è riportato il quadro riepilogativo dello stato di attuazione del programma sopra riportato.

3. RAPPORTO TRA SPESE IN ITALIA E ALL’ESTERO

In totale, per il capitolo 7120-23, sono stati spesi circa **12,8M€** in ambito Nazionale.

² Computer Incident Response Team.

SEZIONE 29

SMD VI - CAP. 7120-27

1. PREMESSA

Ai sensi dell'articolo 548 comma 1 sotto commi b, c, del Decreto Legislativo 15 marzo 2010 n. 66, la relazione riferisce sullo stato di attuazione dei programmi dello Stato Maggiore Difesa – VI Reparto relativi al capitolo 7120-27 realizzati nel 2020.

2. ILLUSTRAZIONE DELLO STATO DI ATTUAZIONE DEI PROGRAMMI

a. Programmi di investimento finanziati con bilancio ordinario

Trattasi di programmi volti ad ammodernare/mantenere/adequare i sistemi di comunicazione e di Comando e Controllo della componente strategica della Difesa e dei Comandi Interforze all'evoluzione tecnologica.

(1) LdB 2017 - Art 1 co. 140 - Terminali Satellitari

Il programma in titolo è finalizzato all'acquisizione di nuove capacità satellitari o all'ammodernamento di capacità già esistenti. Al fine di massimizzare l'utilizzo delle capacità disponibili sul satellite ATHENA-FIDUS, si è reso necessario integrare gli esistenti sistemi di comunicazioni satellitare della Difesa con l'immissione in servizio di alcuni nuovi terminali, o *kit* di adattamento per gli apparati preesistenti, capaci di operare anche in banda Ka. Inoltre sono stati acquisiti alcuni terminali di facile dispiegamento (portabili senza l'ausilio di mezzi). Il programma nel corso del 2020 ha avuto un onere complessivo di 1M€.

b. Quadro sinottico dei programmi

In Tabella 30 al presente allegato è riportato il quadro riepilogativo dello stato di attuazione del programma sopra riportato.

3. RAPPORTO TRA SPESE IN ITALIA E ALL'ESTERO

In totale, per il capitolo 7120-27, sono stati spesi circa 1M€ in ambito Nazionale.

SEZIONE 30

SMD VI - CAP. 7120-32

1. PREMESSA

Ai sensi dell'articolo 548 comma 1 sotto commi b, c, del Decreto Legislativo 15 marzo 2010 n. 66, la relazione riferisce sullo stato di attuazione dei programmi dello Stato Maggiore Difesa – VI Reparto relativi al capitolo 7120-32 realizzati nel 2020.

2. ILLUSTRAZIONE DELLO STATO DI ATTUAZIONE DEI PROGRAMMI

a. Programmi di investimento finanziati con bilancio ordinario

Trattasi di programmi volti ad ammodernare/mantenere/adequare i sistemi di comunicazione e di Comando e Controllo della componente strategica della Difesa e dei Comandi Interforze all'evoluzione tecnologica.

(1) **LdB 2018 – Art.1 co. 1072 – *New Generation Identification Friend or Foe* (NGIFF) - Aggiornamento piattaforme NH-90 e Aggiornamento piattaforme di responsabilità LEONARDO S.p.A.**

Il programma *New Generation Identification Friend or Foe* (NGIFF) si propone di realizzare una capacità che consenta di soddisfare le nuove esigenze operative rappresentate dalla NATO (STANAG 4193 Ed.3 e documento ICAO Annesso 10, fino all'emendamento 85) ed in particolare, quelle relative al passaggio dall'IFF Modo 4 all'IFF Modo 5, attraverso l'aggiornamento dei sistemi (transponder ed interrogatori) ed all'integrazione sulle relative piattaforme aeree, navali e terrestri. In tale quadro, si è reso necessario dare seguito alle attività, intraprese ad integrazione ed aggiornamento della capacità NGIFF delle piattaforme di Forza Armata, allo scopo di adeguare il maggior numero di assetti entro il 2020, secondo le scadenze imposte dalla NATO e dai regolamenti europei sull'aviazione civile. Pertanto, si è dato avvio alle attività finalizzate all'acquisizione dei dispositivi NGIFF e alla integrazione sugli aeromobili NH90, tramite il contratto operante tra l'agenzia della NATO "NAHEMA" ed il consorzio industriale NHI, e alla integrazione sulle piattaforme terrestri e navali di responsabilità Leonardo S.p.A. tramite ulteriore contratto dedicato. Il programma nel corso del 2020 ha avuto un onere complessivo di 1M€, per gli aeromobili della famiglia NHI e circa 10,1M per gli assetti terrestri e navali di responsabilità Leonardo S.p.A.. Le rispettive quote sono state impegnate quasi esclusivamente su territorio nazionale.

b. Quadro sinottico dei programmi

In Tabella 31 al presente allegato è riportato il quadro riepilogativo dello stato di attuazione del programma sopra riportato.

3. RAPPORTO TRA SPESE IN ITALIA E ALL'ESTERO

In totale, per il capitolo 7120-32, sono stati spesi circa **11,1M€**, su territorio nazionale.

SEZIONE 31

SMD VI - CAP. 7120-33

1. PREMESSA

Ai sensi dell'articolo 548 comma 1 sotto commi b, c, del Decreto Legislativo 15 marzo 2010 n. 66, la relazione riferisce sullo stato di attuazione dei programmi dello Stato Maggiore Difesa – VI Reparto relativi al capitolo 7120-33 realizzati nel 2020.

2. ILLUSTRAZIONE DELLO STATO DI ATTUAZIONE DEI PROGRAMMI

a. Programmi di investimento finanziati con bilancio ordinario

Trattasi di programmi volti ad ammodernare/mantenere/adeguare i sistemi di comunicazione e di Comando e Controllo della componente strategica della Difesa e dei Comandi Interforze all'evoluzione tecnologica.

(1) **LdB 2018 - Art 1 co. 1072 - Banca dati unica stipendiali - manutenzione evolutiva e supporto sistemistico**

Al fine di garantire un'ottimale erogazione del servizio ed evolvere il sistema in aderenza alle recenti normative in materia di processi amministrativi e gestionali afferenti al Codice dell'Amministrazione Digitale (CAD), unitamente al Regolamento Generale sulla protezione dei dati (GDPR – *General Data Protection Regulation*), si è reso necessario sviluppare nuove funzionalità *software* con lo scopo di prevedere lo sviluppo di ulteriori funzioni del SIGE, da rendere disponibili all'A.D. secondo i criteri del riuso del SW e che soddisferebbero le ulteriori esigenze di adeguamento prospettate da personale del CUSI e dei centri stipendiali delle F.A.. Tali sviluppi sono mirati a tenere aggiornato il *software* in argomento, in linea con i disposti normativi che dovessero entrare in vigore, nonché a rendere il sistema dell'A.D. pienamente interoperabile con il nuovo sistema stipendiale MEF denominato "Cloudify NoiPA".

Il programma nel corso del 2020 ha avuto un onere complessivo di 1M€.

(2) **LdB 2018 - Art. 1 co. 1072 – Informatizzazione del processo di selezione del personale militare, a perfezionamento dell'iter selettivo psicoattitudinale e della performance individuale e collettiva.**

Per processo di selezione, s'intende "l'insieme di fasi successive, interdipendenti e ben delineate che comprende tre momenti principali: attività preliminari, la valutazione dei candidati e la fase finale, che ha il suo termine con l'arruolamento dei vincitori del concorso".

Nella fattispecie, tale processo è necessario per scegliere i concorrenti che più si avvicinano alle caratteristiche del profilo individuato dalla Forza Armata per ogni categoria a concorso, in modo da garantire standard quantitativi e qualitativi che tendono a livelli di eccellenza del personale che compone lo strumento militare. La fase del processo selettivo che si intende informatizzare è la valutazione dei candidati, in particolare, le prove di efficienza fisica e gli accertamenti fisio-psico-attitudinali, regolate dai bandi di concorso e da apposite direttive tecniche di Forza Armata.

Lo scopo del progetto è quello di ottimizzare l'intero processo di valutazione in termini di:

- introduzione di più moderne metodologie di valutazione e selezione;
- automazione della gestione delle informazioni;

- riduzione dei tempi di lavoro;
- riduzione della possibilità di errore;
- aumento della trasparenza e della sicurezza delle procedure e delle informazioni;
- riduzione dei costi.

Il programma nel corso del 2020 ha avuto un onere complessivo di circa 2M€.

(3) LdB 2018 – Art.1 co. 1072 – Reingegnerizzazione del Portale di Gestione Patrimoniale e Demaniale dell’Amministrazione della Difesa (c.d. Ge.Pa.D.D.).

Nell'ambito del processo di razionalizzazione dei sistemi gestionali della Difesa, in linea con i principi indicati dal Libro Bianco, il Sistema Informativo di Gestione Patrimoniale e Demaniale dell’Amministrazione della Difesa (c.d. Ge.Pa.D.D.) ha consentito alla Difesa di raggiungere diversi obiettivi nella gestione del patrimonio demaniale:

- dotarsi di un Sistema informativo unico per la gestione patrimoniale degli immobili in uso. Il sistema consente il censimento dettagliato di tutti i compendi e permette di associare ad essi dati tecnici, amministrativi (es. utenze di luce, di acqua e di gas) e patrimoniali anche delle strutture presenti all’interno dei fabbricati stessi (es. piani, vani uffici, magazzini ecc.). La disponibilità di un censimento dettagliato di tutte le infrastrutture, consente, inoltre, di associare in maniera univoca sia i pertinenti dati tecnici, amministrativi e patrimoniali afferenti alle strutture stesse sia talune rilevanti specificità di Forza Armata;
- automatizzare i processi riguardanti la gestione e la raccolta dei dati relativi al patrimonio immobiliare in uso, garantendo la rispondenza normativa della gestione delle informazioni (dati generali, geografici, tecnici, catastali, amministrativi, procedure di gestione, concessioni, ospitalità, impianti tecnologici, utenze, lavori, prestazione energetica e verifica sismica);
- consentire ai vari livelli di responsabilità la supervisione, l’inserimento, la modifica, il controllo e la validazione dei dati inseriti dagli organi a cui è affidata la responsabilità della conduzione dei singoli manufatti. La conoscenza di tali informazioni, raccolte in un unico *database*, costituisce un presupposto irrinunciabile per una visione coerente nella definizione delle *policy* di gestione delle infrastrutture.

Il sistema è governato con una specifica direttiva (SMD-I-017) che prevede un *Change Advisory Board* (CAB) preposto ad analizzare le esigenze legate all’utilizzo del sistema (es. rispondenza a modifiche legislative).

Il programma nel corso del 2020 ha avuto un onere complessivo di 0,3M€.

(4) LdB 2018 – Art. 1 co. 1072 – Potenziamiento del Network Access Control dell’Esercito Italiano, della Marina Militare e dell’Aeronautica Militare

Allo scopo di incrementare il livello di sicurezza e controllo in essere sulle reti delle F.A., nonché di rispondere ad un preciso requisito di AgID, si è reso necessario implementare un sistema di controllo degli accessi sugli apparati di *switching multibrand* in uso sulla rete. Detto sistema dovrà integrarsi con WSUS, Antivirus, SIEM e *firewall* attualmente in uso al fine di consentire una più capillare e rapida interpretazione degli eventi, riducendo i tempi di risposta ad eventuali rischi rilevati.

Si è resa, dunque, necessaria una piattaforma di controllo automatico della sicurezza, che consenta di vedere, monitorare e controllare tutto quello che succede sulla rete, tutti i dispositivi, i sistemi operativi, le applicazioni e gli utenti.

La piattaforma si basa su tecnologie di controllo dell'accesso alla rete (NAC) di terza generazione, facile da configurare e che non necessiti di installare *agent* particolari sui terminali.

Il programma nel corso del 2020 ha avuto un onere complessivo di 2M€.

(5) LdB 2018 – Art.1 co. 1072 – Piano di evoluzione strategica del Sistema Informativo Sanitario dell’Amministrazione Difesa (SISAD) - Reingegnerizzazione del Sistema IMAS del SISAM ed integrazione nel SISAD